

UNITED STATES DISTRICT COURT

for the
Central District of California

ORIGINAL

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Case No. 2:18-MJ-867

Nine digital devices seized on March 11, 2018, and currently)
in the custody of the Hermosa Beach Police Department)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the Central District of California
(identify the person or describe the property to be searched and give its location):

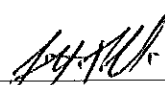
See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the
property to be seized):

See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property. Such affidavit(s) or testimony are incorporated herein by reference.YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance
(not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property
taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the
place where the property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an
inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge
on duty at the time of the return through a filing with the Clerk's Office.
(name)☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay
of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be
searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30).☐ until, the facts justifying, the later specific date of _____.Date and time issued: 4/11/2018 2:15 p.m.
Judge's signatureCity and state: Los Angeles, CaliforniaHon. Alexander MacKinnon, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 12/09) Search and Seizure Warrant (Page 2)

Return		
Case No.: 2:18-MJ-867	Date and time warrant executed: 4/12/2018 4:00 PM	Copy of warrant and inventory left with: Detective Guy Dove, Hermosa Beach Police Dept.
Inventory made in the presence of: Scott Robbins, DSPIS, Beau Stalger - DSPIS		
<p>Inventory of the property taken and name of any person(s) seized:</p> <p>[Please provide a description that would be sufficient to demonstrate that the items seized fall within the items authorized to be seized pursuant to the warrant (e.g., type of documents, as opposed to "miscellaneous documents") as well as the approximate volume of any documents seized (e.g., number of boxes). If reference is made to an attached description of property, specify the number of pages to the attachment and any case number appearing thereon.]</p> <p>Seized approximately 2.6 GB of data from the digital devices including: contacts, SMS messages, iMessages, photos, documents, videos, user data, geo location data</p>		
Certification (by officer present during the execution of the warrant)		
<p>I declare under penalty of perjury that I am an officer who executed this warrant and that this inventory is correct and was returned along with the original warrant to the designated judge through a filing with the Clerk's Office.</p>		
Date: 5/9/2018	<p> _____ Executing officer's signature</p> <p>Scott Robbins Postal Inspector _____ Printed name and title</p>	

ATTACHMENT A

DEVICES TO BE SEARCHED

The following digital devices (the "SUBJECT DEVICES"), seized by the Hermosa Beach Police Department on March 11, 2018, and currently in the possession of Hermosa Beach Police Department:

- a. LG Cell Phone with serial number 608VTRG366510 ("SUBJECT DEVICE 1");
- b. LG Cell Phone with serial number 604CYQX143572 ("SUBJECT DEVICE 2");
- c. LG Cell Phone with serial number 212KPBF1039109 ("SUBJECT DEVICE 3");
- d. LG Cell Phone with serial number 604CYPY187608 ("SUBJECT DEVICE 4");
- e. LG Cell Phone with serial number 405CYF840166 ("SUBJECT DEVICE 5");
- f. Samsung Cell Phone with serial number J727T1UVU7AQD7 ("SUBJECT DEVICE 6");
- g. Grey Toshiba Laptop with serial number [] ("SUBJECT DEVICE 7");
- h. HP Laptop with serial number CND4353JPL ("SUBJECT DEVICE 8"); and
- i. Optima 4GB SD card with serial number 0935WF4570B ("SUBJECT DEVICE 9").

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband fruits, or instrumentalities of violations of Title 18, United States Code, Sections 1029 (Access Device Fraud), 371 (Conspiracy), 1028A (Aggravated Identity Theft), and 1029 (Access Device Fraud) (collectively the "Subject Offenses"), specifically:

a. Data, records, documents, or information (including electronic mail and messages) pertaining to obtaining, possessing, using, or transferring personal and/or financial transaction identification information, such as names, addresses, phone numbers, credit and debit card numbers, security codes, bank account and other financial institution account numbers, Social Security numbers, email addresses, IP addresses, as well as PIN numbers and passwords for financial institutions or internet service providers;

b. Records, documents, programs, applications, or materials pertaining to applications for, or use of, credit or debit cards, bank accounts, or merchant processor accounts;

c. Data, records, documents (including e-mails), or information reflecting or referencing purchases of merchandise, securities, electronic currency, and other valuable things;

d. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written

communications sent to or received from any of the digital devices and which relate to the above-named violations;

e. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications or other text or written communications sent to or received from any digital device;

f. Any documents or records relating to any bank accounts, credit card accounts, or other financial accounts; and

g. Any device used to facilitate the above-listed violations (and forensic copies thereof).

h. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

3. In searching the devices listed in Attachment A (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search the SUBJECT DEVICES for data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search the SUBJECT DEVICES where they are currently located or

transport them to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICES as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in the SUBJECT DEVICES capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICES and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. If the search team, while searching a SUBJECT DEVICE, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of the SUBJECT DEVICE pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that a SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain SUBJECT DEVICE itself if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending),

including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICES, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The special procedures relating to digital devices found in this warrant govern only the search of the SUBJECT DEVICES pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.